

**Faculté des Mathématiques et de l’Informatique**

**Département Informatique**

**Fiche de Proposition PFE Master**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Filière** | Informatique | **Spécialité** | GL |  | R&T |  | GI |  | **Année universitaire** 2018/2019 |

**Encadreur** ……………DAHMANI Youcef…………………………………….

**Grade** ……………………MC classe A……………………………

**Titre du sujet  *……*** L'architecture de paiement electronique 3D-Secure et authentification adaptative pour le Ecommerce***….……..***

**Description du sujet**

Un grand nombre d’internautes utilisent une carte de crédit pour effectuer leur paiement en ligne. De nombreuses architectures de paiement électronique ont vu le jour, à titre d'exemple SET (Secure Electronic Transaction) , C-SET(, Chip-Secure Electronic Transaction), SPA(Secure Payment Application) 3D-Secure. Ces différentes architectures permettent de vérifier l’authenticité des parties concernées par les transactions et l’intégrité des données grâce à l’utilisation de plusieurs algorithmes et protocoles pour assurer :– La confidentialité de l’information et des clés de session via le chiffrement RSA, DES ou 3DES,– un fiabilité et intégrité des données par l’intermédiaire de signatures elctroniques RSA, SHA et HMAC,– et assurer l’authentification du propriétaire de la carte et du marchand par l'usage des certificats X.509 et des signatures RSA. Daans le présent sujet, les candidats sont invités a implementer scrupuleusement l'architecture 3D-Secure et de resepcter son protocol à la lettre. La programmation de la solution client-serveur est à la charge des candidats et doivent prendre en considération les 3 domaines de cette architecture à savoir : 1. Domaine du client - Domaine émetteur (Issuer) 2. Domaine d’interopérabilité - Domaine interbancaire et 3. Domaine du marchand - Domaine acquéreur (Acquirer). La solution implémentée pourrait intégrer selon l'état d'avancement du sujet « Générateur de code à jeton compatible RSA SecurID Token pour Android » l'authentification à 2 facteurs dans le protocol 3D-Secure. Afin de valoriser l'implementation, les étudiants doivent programmer un jeu de sites client serveur pour le Ecommerce. Tous les intervenants doivent être pris en considératio à savoir une site marchand , le client de banque et une API pour les carte bancaires.

**Mots clés** Architecture de paiment electronique , Ecommerce, site marchand, Cryptographie, Authentification forte à deux facteurs, Distribution de clés cryptographiques et certificats électroniques.

**Outils informatiques prévus pour la réalisation :** Un mobile dont le système d’exploitation est Android qui fera office de carte holder, serveurs pour les partenaires des transactions bancaires (banque, sitte martchand) . Le langage de programmation est laissé à l'apprécition des étudiants et peut s’adapter selon leur maitrise (PHP, Java, Android studio, ….). Les candidats devraient avoir des connaissances sur la certification electronique, la cryptographie et la programmation client serveur.

**Plan de travail** Dans un premier temps, les candidats devraient faire 2 études : une étude sur les architecture de paiement electronique, leurs implémentations et leurs modes de fonctionnement (Commande, paiements, autorisation de paiement, ….). Cette étape permettra aux candidats de comprendre le fonctionnement des architectures de paiement via l'internet dans le domaine du Ecommerce. La seconde étude consiste à faire un tour d’horizon sur l'architecture 3D-Secure. Une étude sur ses 3 domaines (Domaine du client - Domaine émetteur (Issuer), Domaine d’interopérabilité - Domaine interbancaire, et Domaine du marchand - Domaine acquéreur (Acquirer)) doit être faite et son protocol de communication doit être maitrisé afin de reproduire cette solution. La seconde phase de ce sujet est l’implémentation d’une solution respectant l'architecture 3D-Secure. Une application client-serveur doit voir le jour en prenant en compte tous les intervenants dans une transaction bancaire à savoir un client, un site marchand, les différentes banques intervenants.

**Références bibliographiques**

1. Cryptographie et Sécurité informatique, Renaud Dumont, Notes de cours, Université de Liège, 2010.
2. https://partnernetwork.visa.com/vpn/app/#!/home

**Signature de l’encadreur**